REMARKS

The Examiner is thanked for the careful review of this application.

Favorable reconsideration and allowance of the present patent application are respectfully requested in view of the foregoing amendments and the following remarks. Claims 1-4, 6-8, 10-15 and 17-25 are pending in the current application. Claims 1, 10, 11, 18, and 19 are independent claims. Claim 25 is added by this Amendment. Claims 5, 9 and 16 are canceled by this Amendment.

Reply to Office's Response to Arguments

Since the Office has maintained the prior rejections and has provided arguments in support of this position, the Applicants will address the Office's response first.

As described at [0079]-[0080] of Koskimies, a secret code is generated for the target device and is made available to the target device and the trusted download server (or data storage system) that is providing the content. Then, the requested content from the trusted download server is encrypted and can only be decrypted by the target device via the use of the secret code (e.g., [0079]-[0081] of Koskimies). Therefore, Koskimies states that "[s]ince content will only work with a single target device, copying the content is of no use" (e.g., [0083] of Koskimies). The requested content is conveyed to the target device from the content server via an SMS or text message (e.g., see [0065] of Koskimies).

The Office is reading a download in compliance with the claimed "predefined security protocol" downloading of the encrypted text message, and is presumably reading a download in non-compliance with the claimed "predefined security protocol" upon an unencrypted text

message. The Applicants note several problems with this interpretation of Koskimies with respect to the claims as amended.

Firstly, independent claim 1 as an example recites "a resident application environment configured to selectively download applications … that comply with a predefined security protocol" and "a download manager … configured to selectively download applications … that do not comply with the predefined security protocol". In Koskimies, whichever module is responsible for receiving text messages handles the text message download, irrespective of whether the text message is encrypted (in compliance with security protocol) or unencrypted (in non-compliance with security protocol). Thus, the *same* target device module handles both types of downloads (any encryption or non-encryption is handled at a higher level), which is different than dividing up the download management of compliant/non-compliant applications between "a resident application environment" and a "download manager" as claimed.

Similarly, in Brody, whether or not a Java applet being downloaded is 'personalized' or not is only ascertained after the download. This teaches away from having different modules (i.e., the "download manager" and "resident application environment") handle downloads of personalized or non-personalized Java applets because the security associated with the Java applet only appears to be evaluated after the fact, i.e., not before the download.

Accordingly, the Applicants respectfully submit that independent claim 1 (and similarly, independent claims 10, 11, 18 and 19) distinguish over Koskimies in view of Brody for at least this reason.

Secondly, independent claim 1 as amended recites "wherein the selectively downloaded applications that comply with the predefined security protocol are executed by the computer platform within the resident application environment, and wherein the selectively downloaded

applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment". This claim language relates to the manner in which the downloaded applications are *executed*; specifically, whether the downloaded applications are executed inside of, or outside of, the resident application environment.

The Applicants have reviewed Koskimies and Davies and submit that their respective teachings relate to whether or not downloaded content is permitted to be accessed at all, but not *where* any execution associated with the downloaded content takes place. For example, in Koskimies, the DRM associated with the downloaded content either prohibits or permits access, i.e., the DRM does not prompt a selection between different execution environments for instance. In Brody, a 'trusted' Java applet is granted full access to resources whereas an 'untrusted' Java applet is not granted full access to resources (e.g., [0022] of Brody). This suggests that the execution of the 'untrusted' Java applet is contained within a subset of the execution environment of the 'trusted' Java applet, and not "outside of" the execution environment of the 'trusted' Java applet.

Accordingly, the Applicants respectfully submit that independent claim 1 (and similarly, independent claims 10, 11, 18 and 19) distinguish over Koskimies in view of Brody for at least this additional reason.

SUMMARY

Since the Office has maintained his rejection of claims 1-24 under 35 U.S.C. § 103 as noted above, the Applicants once again traverse these rejections. The Applicants expressly maintain the reasons from the prior responses to clearly indicate on the record that the Applicants have not conceded any of the previous positions relative to the maintained rejections. For brevity, the Applicants expressly incorporate the prior arguments presented in the 10/11/2010 response without a literal rendition of those arguments in this response.

For at least the foregoing reasons and the reasons set forth in Applicants' response of 10/11/2010, it is respectfully submitted that claims 1, 10, 11, 18, and 19 are distinguishable over the applied art. The remaining dependent claims are allowable at least by virtue of their dependency on the above-identified independent claims. See MPEP § 2143.01. Moreover, these claims recite additional subject matter, which is not suggested by the documents taken either alone or in combination.

For example, claim 25 recites "wherein the predefined security protocol is configured to protect the computer device". In Koskimies, the security protocol corresponds to DRM associated with downloaded content. The purpose of this DRM is to protect the content-owner from illegal distribution or piracy, which is different than protection associated with "the computer device" as recited in claim 25. In other words, Koskimies is not concerned whether to trust malicious software for execution, but rather with whether to trust a user to access content he/she may not have paid for. Accordingly, Koskimies teaches make little sense in context with the recitations of claim 25.

CONCLUSION

In light of the remarks and amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated February 8, 2011

By: /Fariba Yadegar-Bandari/
Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502